https://www.financial-planning.com/news/how-advisors-can-protect-elderly-clients-from-being-scammed

**How advisors can protect older clients from financial scams**
By Rob Burgess
August 30, 2024, 1:34 p.m. EDT

When it comes to scams preying on the elderly, Chris Wilbratte, founder and partner with Echelon Financial in Austin, Texas, is all too familiar.

His assistant's 84-year-old mother was once caught in a sophisticated swindle where the criminals posed as representatives of Publishers Clearing House; their emails even had all the logos from the FDIC, IRS and Federal Reserve Bank.

"It involved multiple calls with the various 'departments' at Publishers Clearing House where they built up their credibility, framed their requests for secrecy and access to investment accounts as part of the normal course of business," Wilbratte said.

What made the con all the more believable was that his assistant's mother had actually won money years before from Publishers Clearing House.

"This seemed even more natural, right?" said Wilbratte. "She won once. Why not? Why couldn't you win twice?"

Scammers targeting vulnerable individuals often pretend to be affiliated with established institutions. (Publishers Clearing House, aware that fraudsters sometimes pose as employees in the hopes of gaining access to winnings, counsels winners to be aware of such grifters.)

In 2023, scams targeting individuals aged 60 and older caused over $3.4 billion in losses — an increase of approximately 11% from the year prior, according to the FBI. And last year, the average victim of elder fraud lost $33,915 due to these crimes.

Experts who have experience dealing with this issue say there are several concrete steps financial advisors can take to defend their mature clients from criminals looking to take advantage.

"I always tell people, 'We cannot prevent fraud, but we can protect against it,'" said Melissa A. Caro, founder of the platform My Retirement Network, a digital media company.

**Sometimes the call is coming from inside the house**
The perpetrators of scams targeting senior citizens are often those closest to them — or those the victims mistakenly think they are close to.

David W. Demming, founder and president of Demming Financial Services in

Aurora, Ohio, said even though his firm is proactive about protecting older individuals, convincing clients they are fraud victims can be difficult. He recalled one 62-year-old client of his who was involved in a romance scam; it ended only after she sent the scammers over a million dollars.

"That was despite our involvement with the family and Schwab's fraud department," he said.

Megan Kopka, managing partner at Apprise Wealth Management in Phoenix, Maryland, is a member of the Cape Fear Elder Abuse Prevention Network. She once had a client whose siblings took their mother, who was in her 90s and had just had surgery, to the bank, where they initiated a withdrawal from her account. They then gave their mom a handwritten IOU note.

"[My] client, who was joint on the account, didn't even get a phone call from the banker with a low six-figure withdrawal," she said. "It's a jungle out there. Adults don't always act like adults."

**Trust but verify**

The first step to making sure older clients are not caught off-guard is coach them on a stance of proactive incredulity, said Noah Damsky, principal of Marina Wealth Advisors in Los Angeles.

For example, financial advisors should instruct clients that when they receive a call from their bank, they should call them back at a number that is publicly listed on the website or the back of their card.

"Banks rarely call customers out of the blue, so any call received should be met with skepticism," he said. "Caller ID can be spoofed, so calling them back at a phone number that is certainly legitimate will ensure they're not talking to a scammer."

Caro said email scammers are getting better at making their fake logos look like they come from real financial institutions.

"I tell folks to never click a link or call a number listed in an email," she said. "Hover over the actual email address it is sent from. Often they are disguised, and that is a dead giveaway."

Todd Rovak is co-CEO and founder of Carefull, a financial safety platform. He said one election-year-specific scam he has seen crop up lately involves political donations, regardless of party affiliation. Advisors can remind clients to always read the fine print to make sure the donation they're making is a one-time gift instead of a recurring one that can drain bank accounts, unbeknownst to the donor.

"They have signed them up, sometimes via text, for this recurring deduction," he said. "Sometimes you see huge amounts coming out."

**Decrease the target area**
Tony Brancato is head of product at Charlie,  a neobank that caters to the 62-plus community. Charlie features a tool that can block all online transactions if the client doesn't do any online shopping.

In June, Charlie also added another feature, called SpeedBump, that can pause payments to all new payees for six hours.

"Someone calls you posing as a grandchild, saying they're in a foreign country," he said. "They've lost their phone. They're in a panic. They're calling from an unfamiliar number, and they need you to send them $500 immediately. … That sense of urgency prompts this victim to send that $500 without even thinking. … An hour later they call the number they have for their grandson and their grandsons there, and they're in America, and they were never in that foreign country. They realize that they've been scammed. That money, they can never get it back. We hear that something like that happens over and over and over again."

There is no right number of financial accounts for a client to own, but the fewer a client has, the easier it is to spot errors or anomalies, said Sean M. Pearson, financial planner at Ameriprise Financial in Plymouth Meeting, Pennsylvania.

"If you have three banks but pay most of your bills from one of them, the lack of activity in the other two may make it more difficult to notice irregularities as quickly," he said. "The best number of accounts for your household is the minimum number of accounts that you need to manage family finances effectively."

Pearson said "boring but simple" steps, like turning on alerts and two-factor authentication, changing passwords and avoiding emailing or texting account numbers and balances, can make a big difference.

"Not all emails and texts are encrypted, and a simple typo could send your information to somewhere that it doesn't need to be," he said. "Technology can be a great tool to make life easier, but like any tool in our toolbox, if we don't use it correctly, we might bang our thumb in the process."

**Secrecy is the enemy**
Wilbratte said what ended up saving his assistant's mother from losing $100,000 was having a trusted contact. The scammers were instructing her to open a new brokerage account and deposit money into it to cover the taxes for her "winnings."

"They would have just taken their money out of the brokerage account with an ACH [automated clearing house]," he said. "When she opened up the new brokerage account, she was being very evasive on the reason why. … The trusted contact was that last line of defense that saved her, from a practical standpoint."

The scammers had anticipated this and had coached the victim to maintain secrecy, said Wilbratte.

"The reason they told her that they needed her to keep the secret is because they don't want to get out until somebody has won something and they can make their large corporate announcement," he said.

Many of these sorts of scams involve an element of secrecy, which is either demanded by the scammers or self-imposed by an embarrassed victim.

"A second set of eyes will help in most situations, be that of a family member or a trusted advisor," said Pearson.